Average-case complexity versus approximate simulation of commuting quantum computations

Michael J. Bremner,[1] Ashley Montanaro,[2] and Dan J. Shepherd[3]

[1] *Centre for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*[*]

[2] *School of Mathematics, University of Bristol, UK*

[3] *CESG, Hubble Road, Cheltenham, GL51 0EX, UK*

We use the class of commuting quantum computations known as IQP (Instantaneous Quantum Polynomial time) to strengthen the conjecture that quantum computers are hard to simulate classically. We show that, if either of two plausible average-case hardness conjectures holds, then IQP computations are hard to simulate classically up to constant additive error. One conjecture relates to the hardness of estimating the complex-temperature partition function for random instances of the Ising model; the other concerns approximating the number of zeroes of random low-degree polynomials. We observe that both conjectures can be shown to be valid in the setting of worst-case complexity. We arrive at these conjectures by deriving spin-based generalisations of the Boson Sampling problem that avoid the so-called permanent anticoncentration conjecture.

Quantum computers are conjectured to outperform classical computers for a variety of important tasks ranging from integer factorisation [1] to the simulation of quantum mechanics [2]. However, to date there is relatively little rigorous evidence for this conjecture. It is well established that quantum computers can yield an exponential advantage in the query and communication complexity models. But in the more physically meaningful model of time complexity, there are currently no *proven* quantum-classical separations.

This can be seen as a consequence of the extreme difficulty of proving bounds on the power of classical computing models, such as the famous P vs. NP problem. Given this difficulty, the most we can reasonably hope for is to show that quantum computations cannot be simulated efficiently classically, assuming some widely believed complexity-theoretic conjecture. For example, any set of quantum circuits that can implement Shor's algorithm [1] provides a canonical example, with the unlikely consequence of efficient classical simulation of this class of quantum circuits being the existence of an efficient classical factoring algorithm. However, one could hope for the existence of other examples that have wider-reaching complexity-theoretic consequences.

With this in mind, recently in both [3] and [4] sampling problems were introduced as a method for potentially proving that quantum computers cannot be classically simulated, assuming the infinite tower of complexity classes known as the Polynomial Hierarchy (PH) [5] does not collapse – an assumption similar to P$\neq$NP. In this approach a classical computer, or sampler, is tasked with approximately mimicking the output of a quantum circuit. That is, it must produce samples from the outputs of the quantum circuit that occur with frequency that is approximately correct. In [3] and [4] it was proven that there is no efficient classical algorithm sampling from quantum circuits to within a small *multiplicative* approximation in each output probability without a PH collapse.

Unfortunately, this notion of approximate sampling is physically unrealistic, as the use of discrete gate sets and the effects of noise induce *additive* errors on quantum computers. As such these results have little physical meaning. It is more reasonable to allow the quantum computer, and its corresponding classical simulator, to sample from a distribution which is close to the desired output distribution in total variation distance (equivalently the ℓ_1 distance).

One important step to addressing this was proposed by Aaronson and Arkhipov in the same work [4], who gave a sophisticated argument based on counting complexity that approximately sampling from the output probability distribution of a randomly chosen network of noninteracting photons (a problem known as Boson Sampling) should be classically hard, even up to a reasonable total variation distance. This major breakthrough rests on two tantalising but as yet unproven conjectures: the so-called *permanent anticoncentration conjecture* and the *permanent-of-Gaussians conjecture*.

In this Letter we propose a generalisation of the Boson Sampling argument of [4] that is native to spin systems. We prove that commuting circuits chosen at random from two well-motivated circuit families inside the class IQP (introduced in [6] and [3]) cannot be classically sampled to within a constant total variation distance, assuming no PH collapse and the IQP equivalent of the permanent-of-Gaussians conjecture. IQP circuits are simple enough to allow us to prove the analogues of the *permanent anticoncentration conjecture*, yet still retain the essential complexity-theoretic ingredients.

Informally an n-qubit IQP circuit $\mathcal{C}$ is a quantum circuit which takes as input the state $|0\rangle^{\otimes n}$, whose gates are diagonal in the Pauli-X basis, and whose n-qubit output is measured in the computational basis [3, 6]. It is often convenient to write $\mathcal{C} = H^{\otimes n}\widetilde{\mathcal{C}}H^{\otimes n}$, where $\widetilde{\mathcal{C}}$ is diagonal in the Pauli-Z basis and H is the usual Hadamard gate. The classically hard IQP circuits in this letter are relatively simple to implement; see, e.g., Figure 1 which corresponds to an Ising model evolution. Implementations are further discussed later in this letter.

The plausible conjectures on which our work is based, stated below, concern the complexity of computing approximations, up to small *relative error*, of output probabilities $|\langle 0|^{\otimes n}\mathcal{C}|0\rangle^{\otimes n}|^2$ of circuits $\mathcal{C}$ that are randomly chosen from circuit families within IQP. We say that A approximates X to within relative error η if $|A - X| \leq \eta X$. One conjecture has an interpretation native to computer science, the other common in condensed-matter physics. Each concerns a quantity

whose approximation up to small relative error is known to be hard to compute in the worst case; the conjecture is that in fact it is just as hard on average. Our main result states that if we assume either of our conjectures, then there is *no way of classically efficiently sampling the outputs of the corresponding families of quantum circuits* without a major re-evaluation of the existing status-quo of complexity theory. More formally:

Theorem 1. *Assume either Conjecture 2 or 3 below is true. If it is possible to classically sample from the output probability distribution of any IQP circuit $\mathcal{C}$ in polynomial time, up to an error of 1/192 in ℓ_1 norm, then there is a BPP^{NP} algorithm to solve any problem in P$^{\#P}$. Hence the Polynomial Hierarchy would collapse to its third level.*

The complexity class P$^{\#\mathrm{P}}$ appearing in this theorem is the class of problems that can be solved in polynomial time given the ability to count the number of solutions of arbitrary NP problems [5]; BPP$^{\mathrm{NP}}$ is the class of problems that can be solved by randomised classical polynomial-time computation equipped with an oracle that can solve any problem in NP.

Our first conjecture is based on the complexity of one of the most commonly studied models of statistical physics, the Ising model. Consider the partition function

$$Z(\omega) = \sum_{z\in\{\pm1\}^n} \omega^{\sum_{i<j} w_{ij} z_i z_j + \sum_{k=1}^n v_k z_k}, \qquad (1)$$

where the exponentiated sum is over the complete graph on n vertices, w_{ij} and v_k are real edge and vertex weights, and $\omega \in \mathbb{C}$. Then, for any $\omega = e^{i\theta}$, $Z(\omega)$ arises straightforwardly as an amplitude of some IQP circuit $\mathcal{C}_I(\omega)$: $\langle 0|^{\otimes n}\mathcal{C}_I(\omega)|0\rangle^{\otimes n} = Z(\omega)/2^n$ (see Supplemental Material [7] and [8–12]). For our purposes it is sufficient to restrict to the case where $\omega = e^{i\pi/8}$ and the weights are picked by choosing uniformly at random from the set $\{0,\ldots,7\}$ on the vertices and edges of the complete graph on n vertices. Our results would still apply for many other choices for ω and distributions on the weights (for example, the edge weights can be picked uniformly from $\{0,\ldots,3\}$), including nonuniform distributions.

The diagonal component of the corresponding circuits $\mathcal{C}_I(e^{i\pi/8})$ can be constructed from $\sqrt{\mathrm{CZ}}$ (square-root of Controlled-Z, i.e. $\mathrm{diag}(1,1,1,i)$), and $T = \left(\begin{smallmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{smallmatrix}\right)$ gates, or alternatively by applying the Ising interaction directly. The number of applications of each gate is given by a simple function of the edge and vertex weights of the associated graph in such a way that random edge weights correspond to a random circuit [7]. See Figure 1 for an example. Let Z_R denote partition functions associated with the uniformly random choice of vertex and edge weights from $\{0,\ldots,7\}$.

Conjecture 2. *It is #P-hard to approximate $|Z_R|^2$ up to relative error $1/4 + o(1)$ for a $1/24$ fraction of instances over the choice of vertex and edge weights.*

A problem is said to be #P-hard if it is at least as hard as any problem in the complexity class #P [5]. It is known that the family of partition functions $Z(\omega)$ parametrised as above

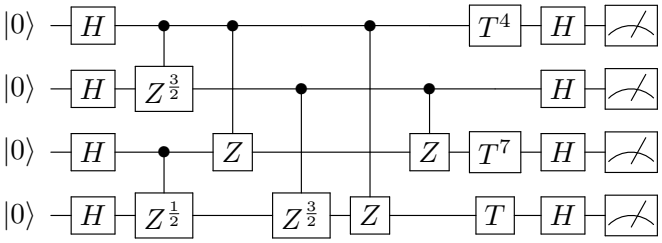

FIG. 1. An example of a randomly chosen circuit $\mathcal{C}_I$ corresponding to a 4-qubit Ising model instance such that $\langle 0|^{\otimes n}\mathcal{C}_I|0\rangle^{\otimes n} = Z_R/2^n$ (up to trivial phase factors). Assuming Conjecture 2 is true, if there exists a classically efficient algorithm for sampling from the output of any such (n-qubit) circuit to within a constant additive error, then the Polynomial Hierarchy collapses.

is #P-hard to compute in the worst case up to the above relative error bound [11, 12]. Conjecture 2 thus states that this worst-case hardness result can be improved to an average-case hardness result.

Our second conjecture is based on the hardness of computing the *gap* of degree-3 polynomials over $\mathbb{F}_2$, $f : \{0,1\}^n \to \{0,1\}$, which are expressible (up to an additive constant) as

$$f(x) = \sum_{i,j,k} \alpha_{ijk} x_i x_j x_k + \sum_{i,j} \beta_{ij} x_i x_j + \sum_i \gamma_i x_i \pmod 2,$$

where $\alpha_{ijk}, \beta_{ij}, \gamma_i \in \{0,1\}$. The gap is defined by $\mathrm{gap}(f) := |\{x : f(x) = 0\}| - |\{x : f(x) = 1\}|$. It can be shown that, for any degree-3 polynomial f, $\langle 0|^{\otimes n}\mathcal{C}_f|0\rangle^{\otimes n} = \mathrm{gap}(f)/2^n$ for IQP circuits $\mathcal{C}_f$ whose diagonal component is constructed from Z, CZ, and CCZ gates for the degree 1-3 terms respectively (see [7]). We write $\mathrm{ngap}(f) = \mathrm{gap}(f)/2^n$. Then we have the following conjecture:

Conjecture 3. *Let $f : \{0,1\}^n \to \{0,1\}$ be a uniformly random degree-3 polynomial over $\mathbb{F}_2$. Then it is #P-hard to approximate $\mathrm{ngap}(f)^2$ up to relative error $1/4+o(1)$ for a $1/24$ fraction of polynomials f.*

It has been known for some time that $\mathrm{ngap}(f)$ is #P-hard to compute exactly in the worst case [13]. We show in the Supplemental Material [7], using IQP techniques, that this worst-case hardness still holds for approximating $\mathrm{ngap}(f)^2$ up to relative error less than $1/2$. Just as with Conjecture 2, what remains is to lift this result to average-case hardness.

The precise values of the constants in Theorem 1 and the above Conjectures are artifacts of the proof technique and can be traded off against each other to some extent: a stronger average-case hardness assumption implies a stronger bound on the difficulty of simulating IQP circuits [7].

That the worst-case complexity of computing $|Z_R|^2$ and $\mathrm{ngap}(f)^2$ is #P-hard up to a constant relative error follows from the fact that the associated gate sets $\mathcal{C}_I$ and $\mathcal{C}_f$ would be universal if we could also perform Hadamard (H) gates at any point in the circuit – which we cannot do in IQP because this gate does not commute with the X gate. However, if we allow the unphysical resource of postselection, these Hadamard

gates can effectively be implemented [3], allowing IQP circuit amplitudes $\langle y|\mathcal{C}|x\rangle$ to express any quantum circuit amplitude (up to a known constant). See Supplemental Material [7] for a description of this construction. This construction also implies worst-case #P-hardness to within exponentially small additive errors [10].

Proving the equivalence of average-case and worst-case complexity is typically challenging, but achievable for certain problems (see [7] for a discussion of this). For example, in [4] there was a direct proof that *exact* evaluation of Boson Sampling probabilities is hard on average. This was based on average-case hardness results for computation of the permanent, for which we do not know IQP analogues. However, currently known techniques do not seem sufficient to extend these exact hardness results for Boson Sampling to approximate hardness results, leading to the *permanent-of-Gaussians conjecture* [4, Section 9.2].

As with the case of Boson Sampling, the worst-case hardness of approximations to both $Z(\omega)$ and $\mathrm{ngap}(f)$ up to small relative error implies via standard results on random-self-reducibility [14] that there exists *some* distribution over the choices of these functions that is #P-hard on average – but not necessarily those required for Conjectures 2 and 3. We believe that our conjectures should hold because there is no structure to the random instances considered that would enable a classical algorithm to solve them more efficiently than in the worst case. In other contexts (such as random k-SAT), there is strong empirical evidence that random instances indeed seem to be hard [15]. Note also our conjectures do not rely on the hard random instances being picked from one particular distribution, but rather the density of hard instances.

Interestingly, recent independent work of Fefferman and Umans [16] has explored an alternative generalization that uses Quantum Fourier Sampling to construct states whose corresponding probability distributions are hard to sample from classically, under similar conjectures to [4]. An appealing aspect of the construction of [16] is that it shows that there are specific, and rather simple, quantum states which are hard to simulate classically, assuming an anticoncentration conjecture holds. However, constructing these states appears to require the full power of quantum computation, unlike the results described here and in [4].

Proof intuition – There are a number of technical ingredients of Theorem 1 which will be discussed below. The basic idea is that, for the class of problems underlying Conjectures 2 and 3, any classical IQP sampler that is accurate up to a good additive error bound in the worst case, is forced to also be accurate to within a reasonable relative error on average. This observation is combined with a classic result of complexity theory, the so-called Stockmeyer counting algorithm ([17] and Supplemental Material [7]), which can be used to estimate individual output probabilities of a classical sampler up to small relative error.

We also use new anticoncentration results for $\mathrm{ngap}(f)$ (for Conjecture 3) and the partition function of the random Ising model (for Conjecture 2). That such anticoncentration results can be proven is a consequence of the elegant mathematical structures upon which IQP circuits are based.

Putting these observations together, we find that there is an $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm for computing a large fraction of $|Z_R|^2$ and $\mathrm{ngap}(f)^2$ values up to small relative error, where FBPP is the functional version of BPP. Assuming the Conjectures 2 and 3, and that the Polynomial Hierarchy does not collapse, this implies that randomly chosen circuits from $\mathcal{C}_I$ and $\mathcal{C}_f$ cannot be classically simulated.

Approximation of general IQP circuits – We first prove a key technical ingredient, which relates approximate sampling from the output distributions of IQP circuits to approximating individual output probabilities. This is essentially the same argument as used in [4] for the permanent, although we believe it becomes substantially simpler in the setting of IQP. The intuition behind this result is that adding random X gates to an IQP circuit randomly permutes the output probabilities. This allows the user of a sampler which is accurate for all circuits to obfuscate from the sampler which one of the output probabilities the user is interested in.

Lemma 4. *Let $\mathcal{C}$ be an arbitrary IQP circuit on n qubits. Let $\mathcal{C}_x$, for $x \in \{0,1\}^n$, be the circuit produced by appending an X gate to $\mathcal{C}$ for each i such that $x_i = 1$. Assume there exists a classical polynomial-time algorithm $\mathcal{A}$ which, for any IQP circuit $\mathcal{C}'$, can sample from a probability distribution which approximates the output probability distribution of $\mathcal{C}'$ up to additive error ϵ in ℓ_1 norm. Then, for any δ such that $0 < \delta < 1$, there is a $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm which, given access to $\mathcal{A}$, approximates $|\langle 0|\mathcal{C}_x|0\rangle|^2$ up to additive error*

$$O((1+o(1))\epsilon/(2^n\delta) + |\langle 0|\mathcal{C}_x|0\rangle|^2/\operatorname{poly}(n))$$

with probability at least $1-\delta$ (over the choice of x).

We prove Lemma 4 in the Supplemental Material [7]. If $|\langle 0|\mathcal{C}_x|0\rangle|^2 = \Omega(2^{-n})$, the algorithm of Lemma 4 gives a good approximation – i.e. an approximation to relative error within roughly $O(\epsilon)$. We state this formally, and calculate the precise constants involved, in [7]. We next show that this condition is indeed satisfied for many circuits picked from two interesting IQP families.

Anticoncentration bounds – Fix a family $\mathcal{F}$ of IQP circuits. We would like to show that $|\langle 0|\mathcal{C}|0\rangle|^2$ is likely to be high for a circuit $\mathcal{C}$ formed by picking a random circuit $\mathcal{D}$ from $\mathcal{F}$, then appending X gates on a uniformly random subset S of the qubits. We will use the following fact:

Fact 5 (Paley-Zygmund inequality)**.** *If R is a non-negative random variable with finite variance, then for any $0 < \alpha < 1$, $\Pr[R \geq \alpha\,\mathbb{E}[R]] \geq (1-\alpha)^2\mathbb{E}[R]^2/\mathbb{E}[R^2]$.*

We will apply Fact 5 to the random variable $R = |\langle 0|\mathcal{C}|0\rangle|^2$, first observing that $\mathbb{E}_{\mathcal{C}}[|\langle 0|\mathcal{C}|0\rangle|^2] = \mathbb{E}_{\mathcal{D},x}[|\langle x|\mathcal{D}|0\rangle|^2] = \frac{1}{2^n}\mathbb{E}_{\mathcal{D}}\sum_{x\in\{0,1\}^n}|\langle x|\mathcal{D}|0\rangle|^2 = \frac{1}{2^n}$, where in the second expectation x is picked uniformly at random from $\{0,1\}^n$. This deals with the numerator; to handle the denominator, we need to upper-bound $\mathbb{E}[|\langle 0|\mathcal{C}|0\rangle|^4]$.

The first family of circuits we consider, $\mathcal{C}_f$, corresponds to polynomials over $\mathbb{F}_2$. We prove in the Supplemental Material [7] that for uniformly random degree-3 polynomials f, $\mathbb{E}_f[\mathrm{ngap}(f)^4] \leq 3 \cdot 2^{-2n}$. Based on this, and the tight connection between IQP circuits over the gate set $\{\mathrm{Z}, \mathrm{CZ}, \mathrm{CCZ}\}$ and degree-3 polynomials, we have the following result:

Theorem 6. *Assume there exists a classical polynomial-time algorithm $\mathcal{A}$ which, for any IQP circuit $\mathcal{C}$, can sample from a probability distribution which approximates the output probability distribution of $\mathcal{C}$ up to additive error $1/192$ in ℓ_1 norm. Then there is an $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm which, given access to $\mathcal{A}$, approximates $\mathrm{ngap}(f)^2$ up to relative error $1/4 + o(1)$ on at least a $1/24$ fraction of degree-3 polynomials $f : \{0,1\}^n \to \{0,1\}$.*

Proof. Combining Fact 5 and the bound on $\mathbb{E}_f[\mathrm{ngap}(f)^4]$, we have $\Pr_f[\mathrm{ngap}(f)^2 \geq \alpha/2^n] \geq (1-\alpha)^2/3$ for any $0 < \alpha < 1$. Fixing $\alpha = 1/2$, we get $\Pr_f[\mathrm{ngap}(f)^2 \geq 2^{-n-1}] \geq 1/12$. The claim then follows from the discussion above (where the precise parameter values stated in the theorem follow from Corollary 3 in [7]). □

We next consider the Ising model, where we are interested in evaluating the partition function Z_R for a randomly weighted graph (see (1)). Recall each edge of the complete graph has a weight w_{ij}, and each vertex has a weight v_k, each picked uniformly at random from the set $\{0, \ldots, 7\}$.

We show in [7] that, up to an easily computed global phase, $\langle 0|\mathcal{C}_I|0\rangle = Z_R/2^n$ for an IQP circuit $\mathcal{C}_I$ whose diagonal component is picked from the set $\{\mathrm{diag}(1,1,1,i), \mathrm{diag}(1, e^{i\pi/4})\}$ (up to trivial phase factors); and further that we can consider a random circuit of this form as being chosen by picking a random circuit using this gate set, then following it by a random choice of X gates. In addition, $\mathbb{E}_{w,v}\left[|Z_R|^4\right] \leq 3 \cdot 2^{2n}$. Via Fact 5 this implies the following result, whose proof is essentially the same as that of Theorem 6:

Theorem 7. *Assume there exists a classical polynomial-time algorithm $\mathcal{A}$ which, for any IQP circuit $\mathcal{C}$, can sample from a probability distribution which approximates the output probability distribution of $\mathcal{C}$ up to additive error $1/192$ in ℓ_1 norm. Then there is a $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm which, given access to $\mathcal{A}$, approximates $|Z_R|^2$ up to relative error $1/4 + o(1)$ with probability at least $1/24$ (over the choice of weights).*

Combining Theorems 6 and 7 gives Theorem 1.

Quantum supremacy and verification – We have argued that the following 'simple' IQP Sampling algorithm should be classically intractable: **(1)** preparing the computational basis state $|0\rangle^{\otimes n}$, **(2)** evolving by a circuit, or equivalent Hamiltonian, randomly drawn from either $\mathcal{C}_I$ (e.g. see Figure 1) or $\mathcal{C}_f$, **(3)** measuring all n qubits in the computational basis, and **(4)** repeating **(1)**-**(3)** polynomially many times. By 'classically intractable' we mean that if this process can be demonstrated in the laboratory, if the total effect of all errors can be demonstrated to remain consistently below 1/192 (in ℓ_1 distance) even as the complexity parameter increases, and if the resources (time) the experiment takes can be argued to grow only polynomially with the complexity parameter, then the process is actively evidencing violation of the extended Church-Turing thesis.

In an IQP experiment that is designed to be hard to simulate classically, the output distribution, while far from the uniform distribution is still rather flat and exponentially many measurement outcomes are possible. Similarly to the case of Boson Sampling [18–20], this implies that verifying that the experiment is working correctly becomes nontrivial: "the task of establishing correct operation becomes one of gathering sufficiently convincing circumstantial evidence" [20]. Two natural experimental approaches towards this are to verify the operation of each gate in the circuit separately, lending confidence that the overall circuit works correctly; or to simulate small experiments classically, to build confidence in the experimental setup before scaling up to classically intractable instances. Verification is assisted by the fact that for IQP circuits, it is always possible to classically estimate any k-local correlation at the output of the circuit [3]. Recent work of Hangleiter et al. [21] describes an approach to verify the output of IQP circuits directly. Finally, previous work [6] has demonstrated that there classes of IQP circuits that admit interactive proof systems where a prover can convince a verifier that he is running an IQP computation versus a classical computation. However, there is no known way of doing this for the random circuits in this paper.

For both the Ising model ($\mathcal{C}_I$) and degree-3 polynomial ($\mathcal{C}_f$) case implementation with commuting gates requires non-local operations potentially between any 2 qubits in the system, which is experimentally challenging. A more viable near-term approach would be to instead implement such circuits via a universal gate set, which would allow implementations via nearest-neighbour gate sets. Likewise, these circuits can also be implemented fault-tolerantly via standard constructions. It is also worth mentioning that there has been significant experimental progress towards implementation of classically difficult IQP circuits. The dynamics of the Ising model with local interactions have been digitally simulated in ion traps [22, 23] and very recently non-local interactions have been utilised in the digital simulation of fermionic systems with superconductors [24]. As technologies such as cavity buses for superconducting systems [25] become more reliable, we expect that an increasing number of systems will be able to implement IQP circuits in a regime that is likely not to be classically simulable.

Outlook – Theoretically there are a number of natural questions that remain to be answered, the most obvious of which is whether or not Conjectures 2 and 3 are true. Recent breakthroughs [26–28] in categorising the complexity of statistical mechanical systems via the underlying interaction graph properties give some hope that these conjectures can be resolved. Extending the connections used here between IQP, the Ising model and low-degree polynomials, to Tutte polynomials and weight enumerator polynomials of binary linear codes [8] is also a compelling direction to be explored.

We would like to thank Aram Harrow, Richard Jozsa, Gavin Brennen, Steve Flammia, and Peter Rohde for helpful discussions and comments on this manuscript. AM was supported by the UK EPSRC under Early Career Fellowship EP/L021005/1. MJB has received financial support from the Australian Research Council via the Future Fellowship scheme (grant FT110101044), and Lockheed Martin Corporation.

* michael.bremner@uts.edu.au

[1] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997), quant-ph/9508027.
[2] I. Georgescu, S. Ashhab, and F. Nori, Rev. Mod. Phys. **86**, 153 (2014), arXiv:1308.6253.
[3] M. Bremner, R. Jozsa, and D. Shepherd, Proc. R. Soc. A **467**, 459 (2011), arXiv:1005.1407.
[4] S. Aaronson and A. Arkhipov, Theory of Computing **9**, 143 (2013), arXiv:1011.3245.
[5] C. Papadimitriou, *Computational Complexity* (Addison-Wesley, 1994).
[6] D. Shepherd and M. J. Bremner, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **465**, 1413 (2009), arXiv:0809.0847.
[7] See Supplemental Material at [] for additional proofs and details, which includes references [29-37].
[8] D. Shepherd, (2010), arXiv:1005.1744.
[9] S. Iblisdir, M. Cirio, O. Boada, and G. K. Brennen, Annals of Physics **340**, 205 (2014), arXiv:1208.3918.
[10] X. Ni and M. Van den Nest, Quantum Information and Computation **13**, 0054 (2013), arXiv:1204.4570.
[11] K. Fujii and T. Morimae, "Quantum commuting circuits and complexity of Ising partition functions," (2013), arXiv:1311.2128.
[12] L. A. Goldberg and H. Guo, "The complexity of approximating complex-valued Ising and Tutte partition functions," (2014), arXiv:1409.5627.
[13] A. Ehrenfeucht and M. Karpinski, "The computational complexity of (XOR, AND)-counting problems," (1990), technical Report 8543-CS.
[14] J. Feigenbaum and L. Fortnow, SIAM Journal on Computing **22**, 994 (1993).
[15] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky, Nature **400**, 133 (1999).
[16] B. Fefferman and C. Umans, "On the power of Quantum Fourier Sampling," (2015), poster presentation, QIP 2015.
[17] L. Stockmeyer, SIAM J. Comput. **14**, 849 (1985).
[18] C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert, "Boson-sampling in the light of sample complexity," (2013), arXiv:1306.3995.
[19] S. Aaronson and A. Arkhipov, Quantum Inf. Comput. **14**, 1383, arXiv:1309.7460.
[20] J. Carolan, J. Meinecke, P. Shadbolt, N. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. Thompson, J. O'Brien, J. Matthews, and A. Laing, Nature Photonics **8**, 621 (2014), arXiv:1311.2913.
[21] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, "Direct certification of a class of quantum simulations," (2016), arXiv:1602.00703.
[22] B. P. Lanyon, C. Hempel, D. Nigg, M. Mller, R. Gerritsma, F. Zhringer, P. Schindler, J. T. Barreiro, M. Rambach, G. Kirchmair, M. Hennrich, P. Zoller, R. Blatt, and C. F. Roos, Science **334**, 57 (2011), arXiv:1109.1512.
[23] J. W. Britton, B. C. Sawyer, A. C. Keith, C.-C. J. Wang, J. K. Freericks, H. Uys, M. J. Biercuk, and J. J. Bollinger, Nature **484**, 489 (2012), arXiv:1204.5789.
[24] R. Barends, L. Lamata, J. Kelly, L. Garca-lvarez, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O'Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, E. Solano, and J. M. Martinis, (2015), arXiv:1501.07703.
[25] J. Majer, J. M. Chow, J. M. Gambetta, J. Koch, B. R. Johnson, J. A. Schreier, L. Frunzio, D. I. Schuster, A. A. Houck, A. Wallraff, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, Nature **449**, 443 (2007), arXiv:0709.2135.
[26] A. Sly and N. Sun, in *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS)* (2012) pp. 361–369, arXiv:1203.2602.
[27] A. Sinclair, P. Srivastava, and M. Thurley, Journal of Statistical Physics **155**, 666 (2014), arXiv:1107.2368.
[28] A. Galanis, D. Stefankovic, and E. Vigoda, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, NY, USA, 2014) pp. 823–831, arXiv:1305.2902.
[29] C. Dawson, H. Haselgrove, A. Hines, D. Mortimer, M. Nielsen, and T. Osborne, Quantum Inf. Comput. **5**, 102 (2005), quant-ph/0408129.
[30] T. Rudolph, Phys. Rev. A **80**, 054302 (2009), arXiv:0909.3005.
[31] S. Fenner, L. Fortnow, and S. Kurtz, J. Comput. Syst. Sci. **48**, 116 (1994).
[32] S. Aaronson, Proc. Roy. Soc. Ser. A **467**, 3393 (2011), arXiv:1109.1674.
[33] A. Bogdanov and L. Trevisan, SIAM J. Comput. **36**, 1119 (2006).
[34] J.-D. Cai, A. Pavan, and D. Sivakumar, in *Proc. 16th Annual Symp. Theoretical Aspects of Computer Science* (1999) pp. 90–99.
[35] M. Jerrum and A. Sinclair, SIAM Journal on Computing **22**, 1087 (1993).
[36] M. Jerrum, A. Sinclair, and E. Vigoda, J. ACM **51**, 671 (2004).
[37] F. Barahona, Journal of Physics A: Mathematical and General **15**, 3241 (1982).